

Cryptography (Day 3)

1. **Progressive Caesar Cipher:** Start with a Caesar cipher, and then shift one letter with each character you are encrypting.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

- (a) Example: Begin with the shift cipher $A \rightarrow Q$, and encrypt the word H E L L O

X V D E I

- (b) Example: Suppose the ciphertext was encrypted with the above scheme. Decrypt the word F R J M S.

P A R T Y

2. **Vigenère Cipher** Choose a keyword, and use that keyword to determine a shift cipher for each letter. (Repeat the keyword over and over.)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

- (a) Example: use the keyword DOG and encrypt the phrase WHERESMYFOOD.

Z V K U S Y P M L R C J

- (b) Example: Suppose the keyword is DOG. Decrypt the ciphertext L Z O N S Y Q C C.

I L I K E S N O W

3. **Double Transposition Cipher:** Use two keywords (often of different lengths). Do a transposition cipher with the first keyword to produce a first ciphertext. If there are spaces, ignore them. Then encrypt that ciphertext (as though it were plaintext) using the second keyword.

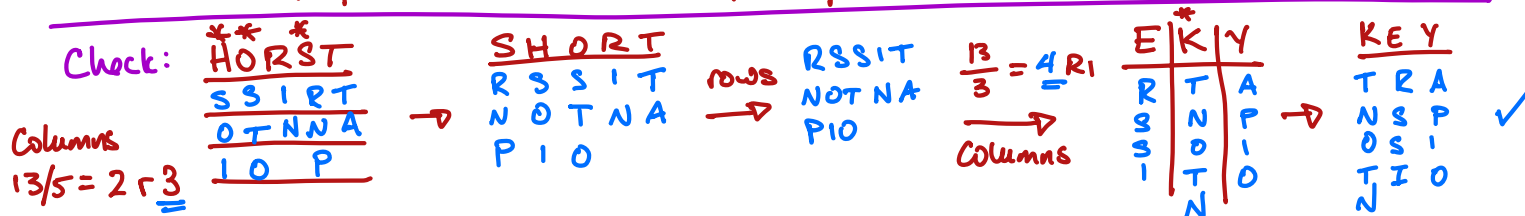
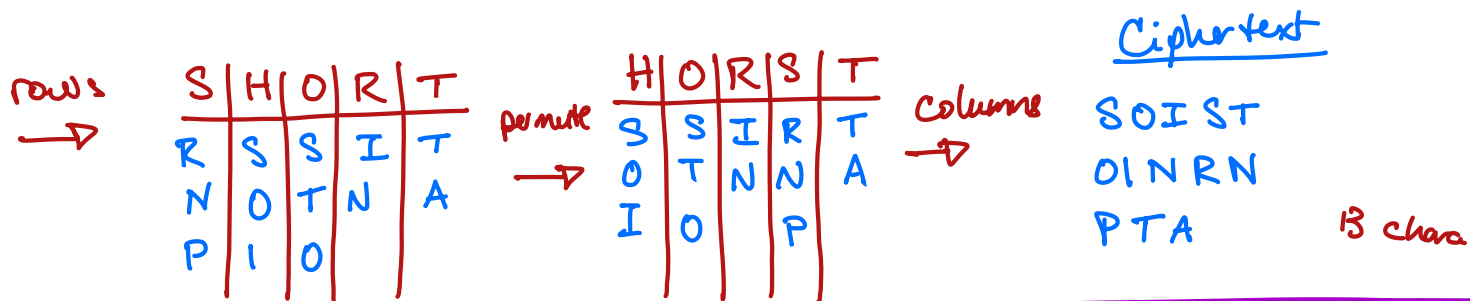
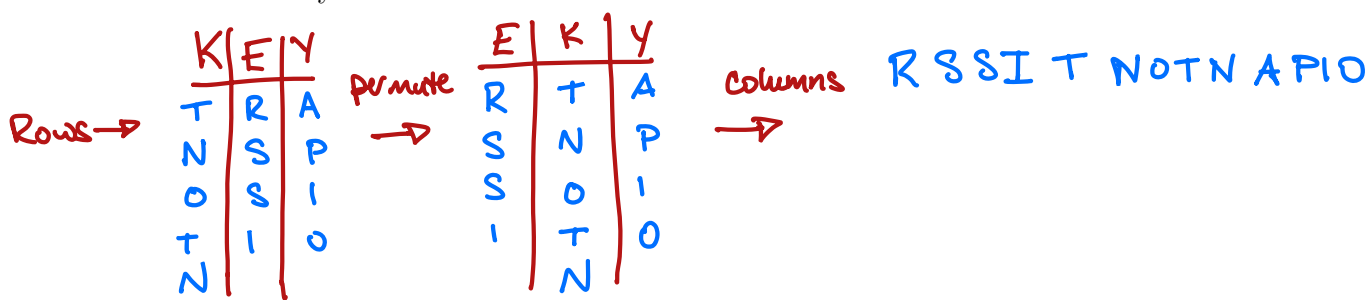
Encryption:

- i. Write the plaintext in rows.
- ii. Permute the columns using the keyword.
- iii. Read off the **columns** to form the new “plaintext”
- iv. Write it in rows in the second grid.
- v. Permute the columns using the second keyword.
- vi. Read off the columns to form the final ciphertext.

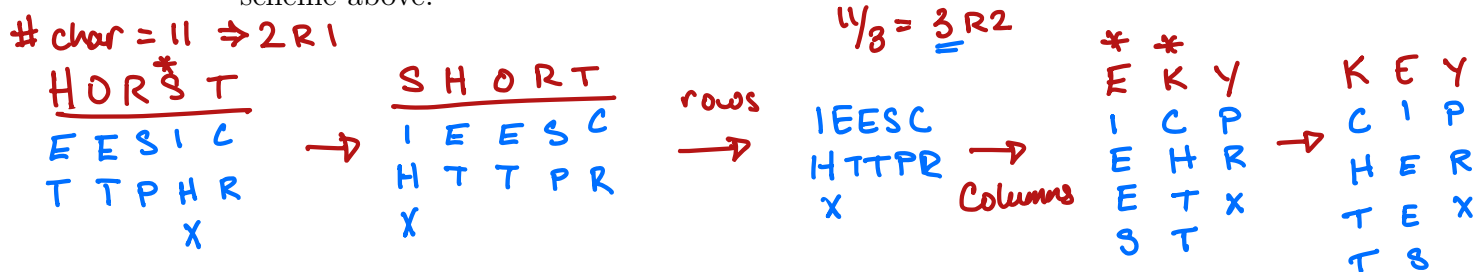
Decryption:

- i. Count the number of characters. Determine how many “extra” characters there will be for the second keyword.
- ii. Write your second grid with the permuted keyword.
- iii. Fill in the columns of the grid, making sure to put the extra characters in the appropriate columns. For example, if your second keyword is **SHORT** and you have two “extra” characters, then columns S and H get one more letter than the other columns. *(Indicate with *)*
- iv. (Un)permute the columns
- v. Read off the rows.
- vi. Using the number of characters, determine the number of “extra” characters for the first keyword.
- vii. Fill in the columns of the grid, filling in the extra long columns using the sorted keyword. For example, if your first keyword is **KEY** and you have two “extra” characters, then columns K and E get one more letter than the other columns.
- viii. Unpermute the columns.
- ix. Read off the **rows**

- (a) Example: Encrypt the word TRANSPOSITION using the first key KEY and the second key SHORT.



- (b) Decrypt the ciphertext ETETS PIHXC R assuming it was encrypted using the scheme above.



CIPHERTEXTS